A Precharge-Absorbed DPL Logic for Reducing Early Propagation Effects on FPGA Implementations

Wei He, Eduardo de la Torre, Teresa Riesgo
Centro de Electrónica Industrial
Universidad Politécnica de Madrid
Madrid, Spain
{wei.he; eduardo.delatorre; teresa.riesgo}@upm.es

***Abstract*—In this paper, a new countermeasure against power and electromagnetic (EM) Side Channel Attacks (SCA) on FPGA implemented cryptographic algorithms is proposed. This structure mainly focuses on a critical vulnerability, Early Evaluation, also known as Early Propagation Effect (EPE), which exists in most conventional SCA-hardened DPL (Dual-rail with Precharge Logic) solutions. The main merit of this proposal is that the EPE can be effectively prevented by using a synchronized non regular precharge network, which maintains identical routing between the original and mirror parts, where costs and design complexity compared with previous EPE-resistant countermeasures are reduced, while security level is not sacrificed. Another advantage for our Precharge Absorbed(PA) - DPL method is that its Dual-Core style (independent architecture for true and false parts) could be generated using partial reconfiguration. This helps to get a dynamic security protection with better energy planning. That means system only keeps the true part which fulfills the normal en/de-cryption task in low security level, and reconfigures the false parts once high security level is required. A relatively limited clock speed is a compromise, since signal propagation is restricted to a portion of the clock period. In this paper, we explain the principles of PA-DPL and provide the guidelines to design this structure. We experimentally validate our methods in a minimized AES co-processor on Xilinx Virtex-5 board using electromagnetic (EM) attacks.**

Keywords-FPGA; SCA (side channel attack); DPL (Dual-rail Precharge Logic); EPE (Early Propagation Effect); LUT; Dual-Core; AES-128

I. INTRODUCTION

Since the introduction by Paul Kocher et al[9], side channel attacks have been considered to be one of the most critical threats to the existing cryptography applications. These attacks get around the extremely time-consuming mathematic computation in conventional cryptanalysis, and directly analyze the physically observable leakages such as power consumption, radiation, timing and even sound.

In this kind of attack, a proper analysis model which is used to predict the physical state of the cryptographic device is constructed. By this model, sensible data could be easily obtained by statistical comparison between the real measured data-dependent variations of these physical leakages and the predicted possible variations.

Another big threat from SCA is due to its furtiveness, since it passively gathers side channel information and therefore leaves very few, or no hint at all, to be detected. Therefore, active protection should always be on duty when the crypto-core is working. Nevertheless, increased energy and resource consumption are concerns, specially for crypto-devices in resource restricted environments, such as WSN (Wireless Sensor Networks), or battery powered devices.

Early Propagation Effect is firstly considered in [1]. The difference of arrival time for the inputs of complementary gates (or LUTs on FPGA) is potential of generating unintentional data-dependent power or EM peaks.

In this paper, we propose a new SCA-hardened countermeasure which is free of EPE. We name it as PA-DPL (Precharge Absorbed-DPL). The merit of our proposal is that it is free of most common drawbacks of EPE-resistant structure. In this proposal, both the precharge and EPE-preventing logic are implemented into the LUT equations. As well, up to 4-input logic gates or functions are permitted with no gate type limitation. Meanwhile, identical routing for true (T) and false (F) rails can be maintained, which is never achieved by previous EPE-resistant countermeasures. In addition, it is possible to save power and area costs by implementing the countermeasures to the cryptographic module using partial reconfiguration.

The rest of the paper is organized as follows. Section II presents the related works of DPL solutions. In section III, we explain the rationale of early propagation and the light-weight countermeasures. Section IV details principles of the proposed PA-DPL. Implementation of a simplified AES co-processor and the experimental results are shown in section V. Finally, we give the conclusions in section VI.

II. RELATED WORK

In SCA, interesting leakages come from the physical level rather than from higher level layer (logic algorithmic level). Accordingly, most countermeasures are deployed at low-level logic layers, i.e. gate level or layout level for reducing or concealing the leakages. Dual-rail precharge logic (DPL) is the typical studied logic protection method. It's experimentally proved to be an effective method towards power, EM and fault attacks. DPL aims to mask physical leakage by compensating the data-dependent power or EM variations. In this structure, a true and a false rail are generated to work in 'evaluation' and 'precharge' cycles periodically. In each evaluation period, the true rail generates true logic values, while the false rail generates the complementary values in each logic cell. The whole system, except the values stored in the memory elements, is forced to be in the precharge state (typically value '0') periodically. DPL mechanism ensures that each complementary gate pair

(compound gate) has one and only one switch in each clock cycle. This method effectively flattens the variations of side channel leakages. DPL is actually a rendezvous of various countermeasures.

As a typical DPL, Wave Dynamic Differential Logic (WDDL)[3] avoids precharging every gate by propagating a wave of value '0'. So, a constrained gate library is needed to provide inverter-free gates. When applied to FPGA based implementations, a compound gate in WDDL cannot assure identical routing for the true and false parts, which inevitably leads to imbalanced side channel leakages[10]. To counter this, MDPL [4] combines the ideas of WDDL and bit-masking to randomly swap the logic interconnect pairs by majority functions, so as to make the circuit insensitive to routing imbalance. Vulnerabilities of masking are revealed in [5][6]. By a so-called Power Density Function (PDF), analysis to a subset of the measurements could remove the masking[20]. DWDDL (Double WDDL)[15] compensates the imbalanced routing by using another WDDL module, but the resource cost is further doubled w.r.t. WDDL.

Early Propagation Effect (EPE) is introduced in [1]. Authors of [2][7][8] prove that the difference of switching time between dual nets of either true or false parts is correlated to the data being processed. All techniques mentioned above suffer from EPE. Some skills are natively or intentionally proposed to resist EPE. Seclib [11] is immune of EPE, but can only be used in ASICs. DRSL[12] ensures synchronized arrival time before the evaluation phase, but not before the precharge phase. STTL [13] introduces a third rail acting as the validation signal to synchronize the inputs. The unique STTL gates are customized which bring troubles to the implementation. An improved structure from MDPL[4], named iMDPL [14], resynchronize all the inputs by inserting SR-Latches. However, the complexity of basic gates is drastically increased.

In [16], a logic structure called BCDL is presented which is capable of resisting EPE by synchronizing all the N pairs of inputs of a compound N-input gate and with no limitation to gate types. It has big decrease of area cost while extra area costs for synchronization logic are still needed. DPL-noEE in [17] avoids the use of synchronization signal by absorbing it into the encoding of LUT functions. In this new LUT encoding, LUT codes for potential intermediate states are modified to make the LUT free of unintentional switching. A pair of 2 input gates can be integrated into 1 4-input LUT and a pair of 3 input gates can be integrated into 1 6-input LUT. DPL-noEE, therefore, is absolutely free of EPE. However routing imbalance for both rails has not yet been solved.

III. Early Propagations and Light-Weight Synchronizations

EPE vulnerability widely exists in conventional DPL structures. When gate switches either from precharge to evaluation phases or from evaluation to precharge phases, EPE potentially occurs in these switching actions. In this section, we detail the rationales of EPE and briefly show the existing light-weight solutions.

A. Difference of Arrival Time

Due to the different logic paths, the arrival times for the different inputs of a gate in ASICs or a LUT in FPGAs are various. A simple gate or LUT doesn't wait for all input values to be in the valid states before it evaluates the output. If the gate type and the combination of the input logic values are proper, an intermediate logic change, normally shown as a peak in power or EM radiation curve, would exist.

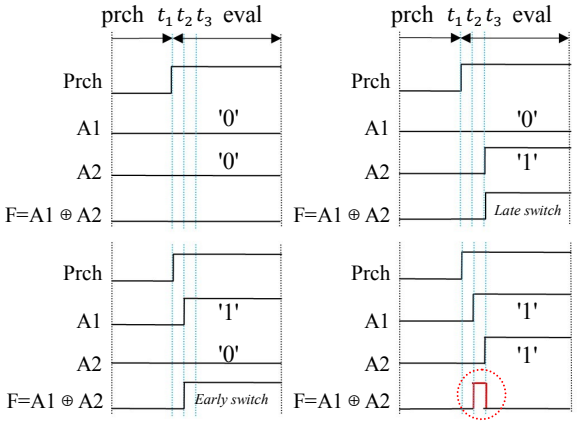

Figure 1. Data-dependent intermediate peak of a 2-input XOR gate.

As shown in Figure 1, a 2-input XOR gate has arrival delays for inputs A1 and A2. The arrival time for the 2 inputs are t_2 and t_3, respectively. At the start of 'evaluation' phase, only when the inputs combination is A1:A2='1:1', an intermediate peak in output F occurs. This peak starts when A1 arrives and ends when A2 arrives. Since it only occurs in proper combination of gate type and input values (Here, XOR gate and A1:A2='1:1'), we could say it's data-dependent. Just by detecting this short peak, we may know what the XOR input values are.

Additionally, just measuring the switching time is also possible to reveal the input value. This attack is based on switching timing delay [8]. In Figure 1, A1 arrives earlier than A2. If output F is evaluated to '1', an early switching action reveals that A1:A2='1:0'; conversely a late one reveals that A1:A2='0:1'. So, switching time is also data-dependent.

In DPL logic, EPE vulnerabilities from different arrival time not only exist within each gate of the complementary gate pair, but also in the counterpart inputs between the gate pair. For example, if the routing lengths for a pair of counterpart inputs are not identical, a power or EM peak is possible as well. As illustrated in Figure 2, with different time delay, peak residues in power or EM curves exist.

The main reason for this delay is the imbalanced routing length of the mainstream DPL logic types on FPGA implementation, where gates are mapped to the LUTs and routing is strictly constrained. In each clock cycle, the register in the previous stage will propagate its memorized value to the register in the next stage. In the propagation through the combinational logic, time is spent mainly in routing wires, switch matrixes connecting each LUT and a small portion to LUT. In ASICs, routing can be properly controlled. In FPGAs, the internal structure of LUTs is a tree

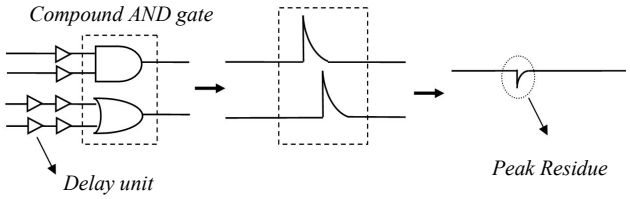

Figure 2. EPE related imbalance of side channel traces in DPL logic.

of multiplexers[16][18]. So, no matter which value is chosen to be output in this configured RAM-LUT, delay time will be constant. That means, LUT delay is generally independent of the input values [19]. Only silicon process variation in the FPGA fabric can spread LUT delay, but if blocks are sufficiently near one to the other, this effect is minimized. Whereas, routing in FPGAs brings big challenges because it can only follow the limited routing resources predetermined by the FPGA structure. It's hard to make complementary routing identical. This introduces big difference in routing length, as shown in Figure 3. Consequently the balances of loading capacitances and arrival delays for the complementary signal pairs cannot be guaranteed in FPGA implementations.

To obtain a DPL structure which is robust against EPE both in precharge and evaluation phases, 2 principles must be followed:

- Within either one of the complementary gates or LUTs, all the input signals should have the same arrival time, or should be synchronized by some mechanisms which make the output of gate or LUT switch only after all the inputs have obtained the valid values.
- Between the inputs of the complementary signal pair, arrival time for them should be identical or should also be synchronized to switch only in valid states.

FPGA gives not much freedom to adopt customized routing planning. Synthesis tools automatically decide where and how to connect the neighboring logic stages. Therefore, special schemes need to be used to eliminate EPE.

B. Light-Weight EPE-Resistant Logic

Cost for countering EPE in DPL is a critical issue. Seclib, STTL and iMDPL are injured by their big expenses on EPE-resistant logic. In recent papers, two light-weight synchronization ways are proposed. One is BCDL which may integrate the synchronization part into the LUTs if limit the input number of the LUT equation to 2. Another one is DPL-noEE which eliminates the intermediate switches due to EPE by modifying the LUT encoding. EPE-free is achieved by modifying the LUT equation to a "monotonic increasing/decreasing function". Any possible intermediate change is avoided by encode it to '0' if precharge state is '0' or to '1' if precharge state is '1'.

Actually, all EPE-resistant logic structure follow the two principles. If they can be obtained, EPE threat is eliminated.

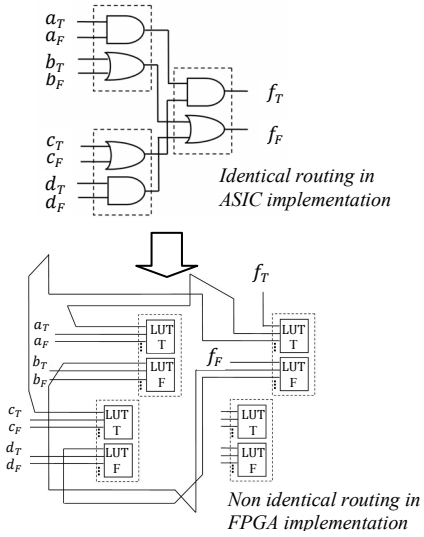

Figure 3. Routing imbalance in FPGA environments.

a) Evaluation phase starts only after the valid value of the slowest input arrives at the gate.

b) The precharge phase starts before the invalid value of the fatest input arrives at the gate.

IV. PA-DPL PRINCIPLE

A. EPE-Free Synchronization

In PA-DPL, precharge signal is reserved but absorbed into a free input of the LUT. Another signal, Ex, is used to act as a synchronization signal working together with 'Prch'. Prch here has doubled the frequency of Ex with a minor time difference advancing Prch, we name it Δ_t. So they could produce a signal $Prch * \overline{E_x}$ which ensures a 25% duty cycle. The signal $Prch * \overline{E_x}$ is just the real precharge signal we use in PA-DPL, as the upper one in Figure 5. Here, one input of an i-input LUT is previously kept free to connect the precharge signal $Prch * \overline{E_x}$.

Figure 4 shows the signal's timing relationships of a PA-DPL 2-input XOR gate when it switches between precharge phase and evaluation phase. In this example, let us suppose that input values of A1:A2 change from '1:1' to '1:0'. A1 arrives the gate earlier than A2. Without Ex, when the inputs move from precharge state '0:0' to evaluation state '1:1', an intermediate transition peak, as shown in Figure 4, would occur. If the gate is precharged by $Prch * \overline{E_x}$, the intermediate peak could be avoided since output would always be in the precharge state '0' unless $Prch * \overline{E_x}$ changes to '1'. This 25% duty cycle ensures that evaluation phase is always late, i.e. evaluation phase only starts after all input signals arrive at the valid states in a permitted frequency range. The minor time ahead of Ex also guarantees that evaluation would ends, i.e. precharge phase starts, before the fastest input arrives at precharge state '0'. This prevents the possible intermediate peak at the start of precharge phase. Furthermore, since the duty cycle of the precharge signal is always precisely 25%, i.e. the switching times of precharge

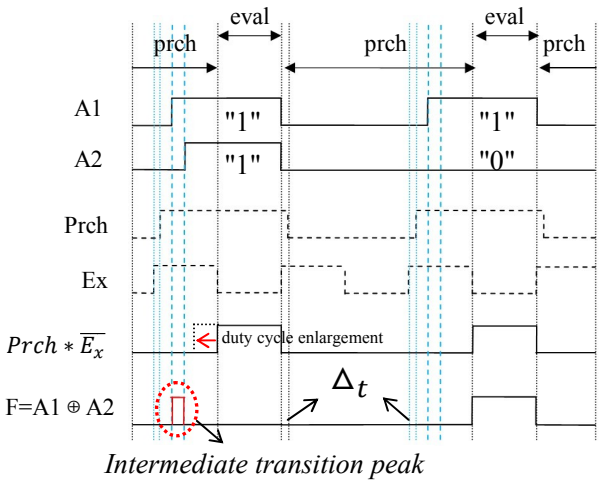

Figure 4. Timing schedule of a 2-input PA-DPL XOR cell.

and evaluation are fixed, the switching timing delay attack [8] previously explained could also be prevented.

By this synchronization technique, inputs for either T gate or F gate is free of EPE both at the start of precharge and evaluation phases. However, if identical routing for T and F parts cannot be assured, the EPE threat still exists for the complementary signal pairs. Therefore, T and F parts should be kept separate in FPGA fabric in order to get the identical routing. This could be done by the "copy and paste" solution used in Divided WDDL [3]. All the information of the true module (including the instances, nets, connections of the original module) is copied and placed to a neighboring fabric (with high regularity) by changing the location parameters. Differing from the technique in [3], we just partially duplicate the module. This step is done by manipulating circuit's XDL description.

B. Precharge-Absorbed Optimization

In PA-DPL, synchronization logic is further absorbed into the LUT equations by using an extra LUT input. This optimization is shown in Figure 5. Since 2 of the LUT inputs are used as the inputs for the synchronized precharge logic, 6-input LUT utilization for mission logic is equivalent to that of a 4-input LUT.

PA-DPL efficiently solves the following major problems:

- In PA-DPL, true and false parts of a compound gate are respectively separated into two parts which preserve precise identical routing for both parts. Due to this merit, the delay time and load capacitance for T and F parts are identical, with the only exception of silicon process variations within the FPGA fabric.
- Gate type is not limited. It is permitted to use any logic gates, considering the LUT size, taking into account that two extra signals are required.
- Masking[4][12][14]: Since the identical routing for both parts are achieved, masking, which is normally used to compensate the routing imbalance of the T and F networks is not required.

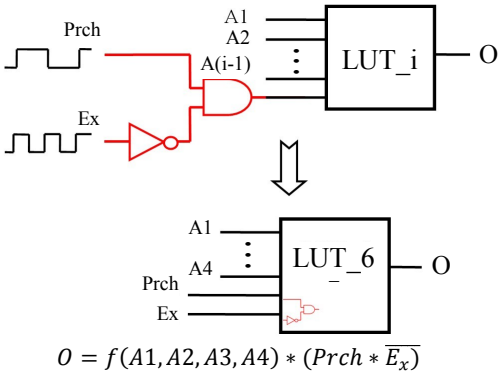

Figure 5. Absorbed synchronization precharge logic in LUT equation.

- Logic complexity is reduced. The design flow can be automatic and requires less effort w.r.t. other solutions.

C. Duty Cycle Enlargement

Actually, the duty cycle of $Prch * \overline{E_x}$ is possibly to be set close to 50%. This can be done by using an Ex with less duty cycle, as shown in Figure 4, $Prch * \overline{E_x}$ can achieve a larger duty cycle. The time difference between the earliest and latest arrival signals is a constant value for a specific design even it works in different speeds. Therefore a larger duty cycle can be applied to a PA-DPL design if it works in low frequency. The expense is that more careful timing managements should be taken in order to ensure the rising edge of $Prch * \overline{E_x}$ will not lag behind the latest arrival signal. Normally, 25% duty cycle provides sufficient design margin and can be easier to be controlled.

V. Implementation and Security Evaluation

A. Implementation on FPGA

A minimized AES co-processor is chosen as the verification target. Figure 6 briefly explains the Dual-Core architecture style, where only the security-sensitive parts (the AES core parts) are protected, and other parts (control logic) are shared by true and false cores. This strategy is helpful in reducing costs (area and energy) in restricted embedded devices. AES-Sbox is implemented by logic elements instead of RAM. The control logic repeatedly runs the encryption of 8-bit pseudo random inputs. A DCM (Digital Clock Manager) is used to generate the Ex from Prch meanwhile gives a constant time delay 'Δ_t' (by setting fine-grained phase shifting). Other timing delay logic could be used as well if the frequency drops out of the permitted frequency range of DCM.

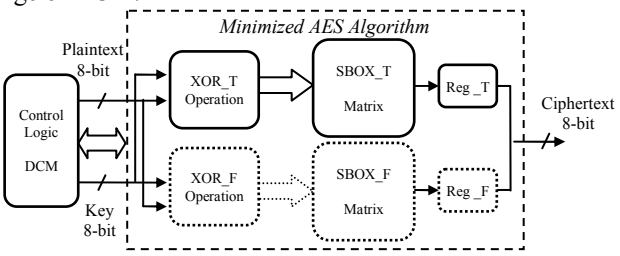

Figure 6. Dual-core architecture of a minimized AES module.

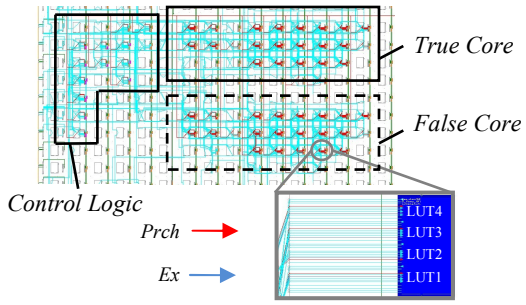

Figure 7. PA-DPL implementation of a minimized AES module.

Implementation on Virtex-5 FPGA is presented in Figure 7. The false module is deployed in a location very close to the true module. They share the same control logic and the synchronization precharge network. Virtex-5 FPGA series have LUTs with 5 or 6 inputs. Therefore, except the 2 inputs used for the synchronization precharge logic, the other 4 could be used for any 4-input Boolean functions. Precharge network reaches every LUT. Hence, all cells can be precharged simultaneously.

Experiments show that if we randomly choose a pair of signals from T and F modules respectively, they compensate with each other precisely following the principle of DPL, but differing for the 25% evaluation time during each clock cycle, as illustrated in Figure 8. Because the valid values can only take evaluation time to propagate to the next registers. A 25% evaluation time in PA-DPL inevitably requires a slower clock frequency to meet the timing requirement of the critical path. Nevertheless, PA-DPL has more freedom in logic optimization which helps to get a shorter critical path. Therefore, it effectively mitigates the timing pressure due to shorter evaluation time.

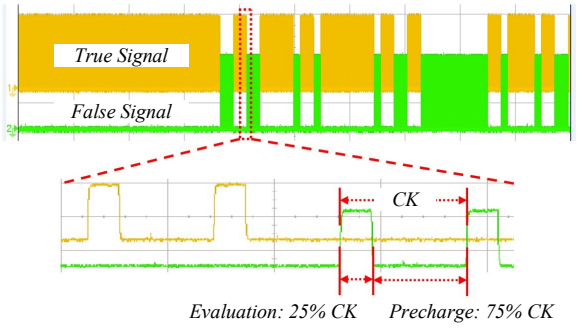

Figure 8. Complementary and precharged signal pair using PA-DPL.

B. Security Evaluation and Attack Results

An EM attack platform was set up to evaluate the security level of the PA-DPL against differential EM attacks. Similar attacks to a SE (Single Ended, i.e. Unprotected) one and a WDDL one are also done in order to make the comparisons. They are implemented in similar fabric position on a Xilinx Virtex-5 FPGA. We tested the circuit at frequencies from 844KHz to 33MHz. The maximum frequency reaches to 104.8MHz in timing analysis. EM traces are gathered by a self-made multi-turn copper antenna. Results show that the right key is differentiated from the wrong keys by analyzing merely 400 traces in the attack to

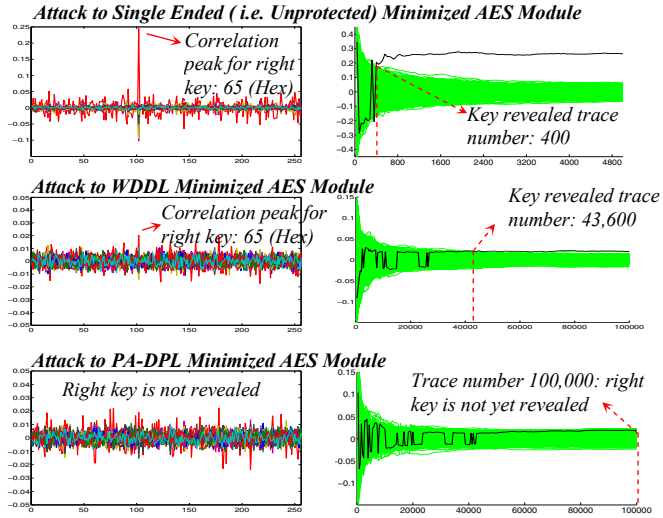

Figure 9. Experimental attacks to 3 implementations: 1) Single Ended; 2) WDDL; 3) PA-DPL.

SE. WDDL resists attack until trace number reaches to 43,600. Comparatively, the key has not yet been differentiated even we increase the analyzed traces to 100,000, gaining an increase factor of robustness at least 250 from SE one, and a factor at least 2.3 from generic WDDL. Correlation peaks are plotted in Figure 9.

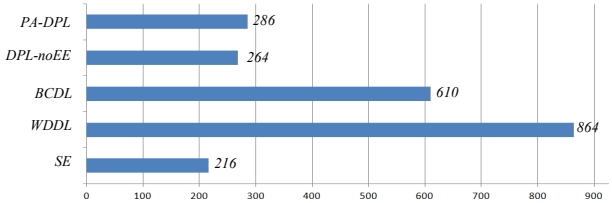

Figure 10. LUT costs for different implementations on Virtex-5 FPGA.

C. Cost Comparisons

Compared with other FPGA implemented EPE-resistant DPL approaches, PA-DPL gives strong protections against EPE-related side channel threats meanwhile keeps minimum resource overheads. We give a comparison showing LUT occupations of our method and several other published solutions. Since there are 4 LUTs available in each Virtex-5 SLICE, we can constraint 2 compound gates to one SLICE in WDDL implementation. For BCDL and DPL-noEE, results are estimated by counting the number of 2-input or 3-input gates synthesized from ASIC gate-limited library. For instance, in Synopsys Design Compiler, we use '*set_dont_use*' attribute to all the gates except the 2-input ones in BCDL estimation and 2/3-input ones in DPL-noEE estimation. The gate numbers from the 2 gate-level netlists are the numbers of LUT costs for BCDL and DPL-noEE estimations respectively. Comparison results show that in Virtex-5 environment, PA-DPL is the second best one in LUT occupation, only a little larger than DPL-noEE. And it has the best performance in avoiding imbalanced routing due to the routing identity between T and F cores.

TABLE I. CHARACTERISTIC COMPARISONS OF DIFFERENT SCA-HARDENED TYPES IMPLEMENTED IN VIRTEX-5 FPGA ENVIRONMENT

Countermeasure Types	EPE free		Routing Identical	Precharge Networks	Optimization Possibility		EPE-Synchronization Logic Size
	Prch	Eval			Gate type	Maximal Permitted Gate Inputs	
SE	*	*	*	*	*free*	*Free**	*
WDDL	×	×	*No*	*Small*	*Inverter Forbidden*	*Free**	*
DRSL	×	√	*No*	*Small*	*free*	*2*	*Large*
iMDPL	√	√	*No*	*Medium*	*Inverter Forbidden*	*2*	*Very Large*
BCDL	√	√	*No*	*Large*	*free*	*Rendezvous is separate: free* *Rendezvous is integrated: 2*	*Medium*
DPL-noEE	√	√	*No*	*Small*	*free*	*2 (in 4-input LUT)* *3 (in 6-input LUT)*	*Small*
PA-DPL	√	√	*Yes*	*Large*	*free*	*4 (in 6-input LUT)*	*Small*

* **free*** in "Maximal Gate Inputs" depends on specific devices.

VI. CONCLUSIONS

In this article, we presented a new SCA-hardened structure which aims to solve the vulnerabilities of EPE and imbalanced routings, meanwhile keeping smaller cost compared with other EPE-resistant DPL methods. This is summarized in Table I. High efficiency in resource costs benefits from the permission of using any gate type and as more as 4 inputs (for FPGA with 6-input LUT). Partial implementation of the countermeasure further helps to save the hardware and power costs. We implemented a minimized AES module by our countermeasure in Virtex-5 FPGA environment and made comparison attacks to unprotected and WDDL ones. Experimental results in our tests show that PA-DPL has increased robustness of at least a factor of 250 from the unprotected one and a factor of 2.3 from WDDL, with a minimum area cost w.r.t. most previously published EPE-resistant countermeasures. Separate architecture for true and false parts makes PA-DPL well suited for partial dynamic reconfiguration, which makes it potentially to be used in reconfiguration based dynamic security protection.

A trade-off is the shorter evaluation time which restricts the maximal speed. However, a bigger opportunity of logic optimization in PA-DPL helps to shorten the critical path. Further timing optimization and real time reconfiguration of the false core would be a part of the future work.

ACKNOWLEDGMENT

This work was partially supported by the Artemis program under the project SMART (Secure, Mobile Visual Sensor Networks Architecture) with number ARTEMIS-2008-100032.

REFERENCES

[1] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using Dual-Rail Pre-Charge logic style," in CHES, LNCS, vol. 4249. Springer, 2006, pp. 255-269.

[2] K. Kulikowski, M. Karpovsky, and A. Taubin, "Power attacks on secure hardware based on early propagation of data," in IOLTS, IEEE, Computer Society, pp. 131-138, July 2006.

[3] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in DATE'04. IEEE Computer Society, Paris, France, pp. 246-251, Feb 2004.

[4] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in CHES, LNCS, vol. 3659. Spring, pp. 172-186, Edinburgh, Sco, UK, Sep 2005.

[5] K. Tiri and P. Schaumont, "Changing the odds against masked logic," Proc. 13th International Workshop Selected Areas in Cryptography (SAC 06), LNCS 4356, Springer, 2007.

[6] P. Schaumont and K. Tiri, "Masking and dual-rail logic don't add up," in CHES, LNCS, vol. 4727. Springer, pp. 95-106, Sep 2007.

[7] D. Suzuki and M. Saeki, "An analysis of leakage factors for dual-rail pre-charge logic style," IEICE, Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E91-A(1): 184-192, 2008, doi: 10.1093/ietfec/e91-a.1.184.

[8] S. Guilley, S. Chaudhuri, L. Sauvage, T. Graba, J.-L. Danger, P. Hoogvorst, V.-N. Vong, and M. Nassar, "Shall we trust WDDL?" in Future of Trust in Computing, vol. 2, Berlin, Germany, Jun 2008.

[9] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," Proc. Cryptology (CRYPTO 99), LNCS, vol. 1666, pp. 388-397, Aug 1999.

[10] S. Guilley, S. Chaudhuri, L. Sauvage, T. Graba, J.-L. Danger, P. Hoogvorst, V.-N. Vong and M. Nassar, "Place-and-route impact on the security of DPL designs in FPGAs," in HOST, pp. 29-35, IEEE computer Society, June 2008.

[11] S. Guilley, F. Flament, R. Pacalet, P. Hoogvorst, and Y. Mathieu, "Security evaluation of a balanced quasi-delay insensitive library," in DCIS, Grenoble, France, Nov 2008.

[12] Z. Chen and Y. Zhou, "Dual-Rail random switching logic: a countermeasure to reduce side channel leakage," in CHES, LNCS, vol. 4249. Springer, 2006, pp. 242-254, Yokohama, Japan.

[13] R. Soares, N. Calazans, V. Lomné, P. Maurine, L. Torres, and M. Robert, "Evaluating the robustness of secure triple track logic through prototyping," in SBCCI, NY, USA: ACM, pp. 193-198, 2008.

[14] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the maked logic style MDPL on a prototype chip," Proc. Cryptographic Hardware and Embedded Systems (CHES 07), Vienna, Austria, Sep 10-13, 2007.

[15] P. Yu and P. Schaumont, "Secure FPGA circuits using controlled placement and routing," Proc. 5th IEEE Hardware/Software Codesign and System Synthesis, NY, USA: ACM, pp. 45-50, 2007.

[16] M. Nassar, S. Bhasin, J.-L. Danger, G. Duc, and S. Guilley, "BCDL: a high speed balanced DPL for FPGA with global precharge and no early evaluation," in Proc. Design, Automation and Test in Europe (DATE 2010), pp. 849-854, IEEE Computer Society, Dresden, Germany, Mar 2010.

[17] S. Bhasin, S. Guilley, F. Flament, N. Selmane, and J.-L Danger, "Countering early evaluation: an approach towards robust Dual-Rail precharge logic," in WESS. ACM. Oct 2010. Arizona, USA. doi: 10.1145/1873548.1873554.

[18] D. Suzuki, M. Saeki, and T. Ichikawa, "Random switching logic: a countermeasure against DPA based on transition probability," Cryptology ePrint Archive, Report 2004/346.

[19] Virtex-5 FPGA User Guide, Xilinx, UG190 (V5.3), May 2010.

[20] E. Mulder, B. Gierlichs, B. Preneel, and I. Verbauwhede, "Practical DPA attacks on MDPL," Cryptology ePrint Archive, Report 2009/231, May 2009.